gig economy workers and for those who are now benefiting from the Federal extension, the 13-week extension, but also additional funding. My understanding is direct payments are also in the mix.

I just wish they would get their work done. It has been 9 months since the CARES Act was done. I just hope we can figure out a way to get through the hurdles that remain. I have spent much of the day—as have my colleagues, I am sure—talking to colleagues, trying to figure out how to fix the last couple of issues that apparently are out there. But my hope is that even if it is not a perfect bill for me—and it won't be. I know it won't be. We spent 3 or 4 weeks working on legislation that is bipartisan that isn't what any of us would have crafted individually, but it provides that needed help right now. We need it both for the economic crisis that has been caused by this virus but also the healthcare crisis, which, unfortunately, is getting worse in my home State of Ohio and not better.

The vaccine is on its way. That is very exciting. I believe that the vaccine development and now the distribution are actually quite impressive. I think the administration deserves credit for that, as do so many hard-working scientists who have been sleeping in their offices, making sure that we have this vaccine available. But there is going to be a bridge here. There is a time period between now and March and April when it is not going to be readily available to everybody we represent. During that time period, we need a bridge. We have needed it for a while, so my hope is we will get that done tonight.

TRIBUTE TO TERESA SIMMS

Madam President, I also want to mention briefly, I just came in on the underground subway from the offices and ran into a woman who has spent 41 years working here for us—one of those selfless, hard-working employees of the United States Capitol. Her name is Teresa Simms. Many of you know Teresa. She always has a smile on her face. She is always optimistic. She always has a focus on providing the best service to all of us—staff, other employees, Members. She started in the cafeteria. She then went to the night cleaning crew, cleaning offices here in this place at night. And then she was promoted to being one of the drivers of the subway. For 41 years, again, she has done that job dutifully, with great commitment.

She is going to retire and spend more time with her family and, particularly, take care of her mom, who is ill. Tonight we want to offer our thanks and gratitude to her and our best wishes to her in retirement.

GOVERNMENT FUNDING

The other thing that is going on tonight—I will say, I guess it is obvious—is that we are about to hit the government shutdown time period again. I mean, we are only about 6½ half hours from another government shutdown. That is totally unacceptable. We should never have these shutdowns. They don't make any sense. By the way, to my Republican friends who think these shutdowns are good because you shut down a lot of government, and it seems like you would save money—we never save money. The taxpayers always pay more. You go back and provide backpay even for services that aren't provided.

I think we have to figure out a way, when we can't get our work done here—and that is why this is happening. We have not gotten our spending bills, appropriations done here. Therefore, we are facing a government shutdown again. At midnight, we turn into pumpkins. It means the government starts to get shut down.

By the way, it creates confusion and uncertainty for Federal workers, of course, who are wondering, are they going to have their job and are they going to get paid, but also confusion and uncertainty for a lot of citizens who are depending on the services that would otherwise be provided. It is so inefficient. If you believe in the efficiency of government and you believe in, you know, not wasting money, you shouldn't want these government shutdowns.

My hope is that we do pass a continuing resolution at least to kick us into the next couple of days so that we don't have a shutdown tonight. That would be such a disaster for so many people. And it could last a long time, by the way, as these shutdowns did over the last couple of years. It doesn't just mean it is a few days. Let's just not go into shutdown at all.

I have introduced legislation called End Government Shutdowns for 10 years now. I have introduced it in five different Congresses. We have 33 cosponsors. I think it has more cosponsors than any other bill like it, but there are other ideas out there, and I am open to them—just some way to get away from these shutdowns. Our bill says you just can't shut it down. When you are going for a shutdown, instead, you just do a continuing funding from the previous year. And then, by the way, over time, you reduce that by 1 percent every 90 days and every 60 days to get the attention of the appropriators to get them back to work. Other people have other ideas. Our bill has been bipartisan in the past. I don't believe it is today, but it does have 33 cosponsors.

My hope is that we can figure out a way to end these government shutdowns with simple legislation that says: Let's just not do it. I don't think it provides healthy leverage. I think it provides, again, uncertainty and confusion.

CYBER SECURITY

Madam President, 2020 has been a tough year, let's face it. And, unfortunately, it looks like the challenges haven't ended. I came to the floor tonight, primarily, to talk about some shocking and disturbing news we just heard over the last few days, and that is that there has been a massive, highly sophisticated, and ongoing cyber attack that has compromised the networks of multiple Federal agencies and the private sector.

According to reports, for months now—months—hackers—our intelligence experts think they are most likely connected with the Russian Government in some way. That is what they tell us. But these hackers have engaged in an espionage effort to access information in some of our biggest Federal agencies that hold some of our most sensitive data and our most sensitive and important national security secrets.

Also, again, many U.S. private companies were hacked, as well. These hackers are smart. They targeted some of these agencies that do handle things like national security—the State Department, for instance, the Department of Homeland Security, the Department of Energy and its Nuclear Security Administration.

This is scary stuff. Others, like the National Institutes of Health, were hacked. Of course, they are closely involved with our work to respond to the COVID–19 pandemic, so also a lot of important, sensitive information could have been hacked. They are a treasure trove of information. These are agencies that protect our homeland, promote our freedom abroad, and are on the frontlines battling this pandemic.

But what we know today may be just the tip of the iceberg, we are told. Experts expect the number of agencies as well as a number of private companies victimized by this attack will only continue to grow.

The main IT monitoring platform believed to have been hacked was used across the government and by 33,000 private companies. Shockingly, we also know that FireEye, the preeminent cyber incident response firm, was also breached. So think about this. FireEye, which is a company that people call when they are hacked, was hacked.

We are still learning the details about this attack, but what we know is chilling. Federal investigators from the Cybersecurity and Infrastructure Security Agency, CISA, under the Department of Homeland Security, the FBI, and also the Office of National Intelligence, the ODNI, are all working to determine how this happened, what the extent of it is.

But it looks like the main vulnerability was through a SolarWinds' platform, which is an IT monitoring platform widely, again, widely used by the government and the private sector to oversee the operation of other computer networks.

The hackers disguised their entry into these Federal agencies and company systems in a troubling and clever way. They exploited a vulnerability in a security patch sent out by SolarWinds to update its software. I want to emphasize that—the security patches that we all advocate to be installed as soon as possible to protect

our networks as basic good cyber hygiene was actually a security breach.

This technique and the breadth of this hack are both unprecedented, and it shows that the Federal Government is still far from where we need to be to handle the cyber security challenges of the 21st century.

As the Permanent Subcommittee on Investigations said in its investigation and report, these alarms that we have been raising over time are ones that we should have paid attention to. In 2019, last summer, Senator CARPER and I issued a shocking report that detailed the unacceptable cyber security vulnerabilities in the Federal Government—vulnerabilities that may very well have played a role in the extent of this breach.

Our report looked back at how well Federal agencies complied with basic cyber security standards over the past decade. Every agency we reviewed failed. And we know that four of those agencies—the Department of Homeland Security, the State Department, the Department of Agriculture, the Department of Health and Human Services—are among those that have been breached in this current cyber attack.

That report from the Permanent Subcommittee on Investigations made clear that Federal agencies were a target for cyber criminals and other nation-state adversaries. In 2017 alone, Federal agencies reported 35,277 cyber incidents. It is the most recent data we have—in 1 year. The number of cyber incidents in 2019 was a little bit less, 28,581. But 2020 will bring what is likely the biggest, most comprehensive breach across the Federal Government in our history.

We also found we are not equipped to handle this threat. Many of the agencies we reviewed didn't even know what applications and platforms were operating on its systems. That begs the question: How can you protect something if you don't even know what you need to protect?

If Federal agencies fail at meeting basic cyber standards, there is no way they are equipped to thwart the kind of sophisticated attack that apparently happened over the past several months. Here, the attackers were meticulous and had a detailed understanding of how to evade intrusion detection practices and technologies. And because the Federal agencies involved were unprepared, the attackers had ample time to cover their tracks, which means evaluating the extent of the damage and kicking them off our networks is going to be incredibly difficult and time-consuming.

Given how widespread this attack is and how much wider it is expected to become, it certainly seems like the Federal Government's current cyber resources are going to be spread incredibly thin.

Congress and the executive branch have failed to prioritize cyber security, and now we find ourselves vulnerable and exposed. We have to do better than this. This breach has to be a wake-up call for all of us.

Over the years, I have worked across the aisle with Senator PETERS, Senator CORNYN, Senator HASSAN, and others on legislation to beef up our Federal Government cyber capacities, including the Risk-Informed Spending for Cybersecurity Act, the Federal System Incident Response Act, and the DHS Cyber Hunt and Incident Response Team Act, and others. We are proud of this legislation.

Let's be honest. It wasn't enough. We need to do more. We need to not only defend our networks but go on the offense to defer a nation-state, like Russia, and nonstate actors from even considering a future attack like this. That means there needs to be consequences for cyber attacks significant enough to prevent them from happening again and a willingness to act preemptively when warranted.

Congress has to take a hard look at the cyber security capabilities of our Federal agencies. In the next Congress, I will be the top Republican on the Senate Homeland Security and Governmental Affairs Committee, which means I will either serve as its chairman or ranking member, depending on the outcome of a couple of races in Georgia. Senator PETERS will be the chair if the Democrats take the majority. I will tell you here tonight, whether I am chairman in January or him, we intend to hold indepth hearings on cyber security. With what has happened, we will also, of course, focus on the origin, scope, and severity of this breach.

Actually, 3 weeks ago, even before this attack was revealed, we met and decided to hold these cyber security hearings, and we are already working on comprehensive legislation to improve our cyber defenses in the Federal Government going forward.

We must now move with a renewed sense of purpose and urgency to learn from this massive attack. We have to remove these hackers from these systems and put in place protections to prevent it from happening again.

As this cyber attack has made clear, we have to redouble our efforts to shore up our defenses. We are two decades into the 21st century, but most of the Federal Government legacy computer systems are from the 20th century. Federal agencies are simply behind the times when it comes to defending themselves against these threats posed in cyber space. The government is trying to respond to sophisticated, 21st century attacks with 20th century defenses. This attack has shown us the consequences of that and should be the catalyst for real bipartisan action here in the next Congress to better defend networks that contain sensitive, personal information, and other information critical to our economy, our healthcare, and the safety and security of all Americans.

I yield the floor.

The PRESIDING OFFICER (Mr. TILLIS). The Senator from Ohio.

Mr. PORTMAN. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. BENNET. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

CORONAVIRUS

Mr. BENNET. Mr. President, before I give my remarks, I would like to say that I hope the rumors are true that we are getting close to a deal here. The country needs us to reach a bipartisan deal, as we did in March, unanimously, when we passed the CARES Act here.

It is time for us to do that again. In Colorado and all across the country cases are spiking and the economy is slowing down. People need relief. They need help. I hope we will come together in a bipartisan way and do that.

I hope that the deal is not going to come crashing down because of a disagreement about what the Federal Reserve's authority ought to be under the 13(3) program. That is an important program for the Federal Reserve to help when things are really distressed in our economy—to help our small businesses, our State and local governments, and working families all over this country.

It is an authority that Donald Trump used—or that the Fed used while Donald Trump was President. People on both sides of the aisle said it was an effective authority, and if it is an effective authority for President Trump, it should not be taken away from the Federal Reserve just because Joe Biden is becoming President of the United States.

So I hope that we will come to an agreement. I expect that we will. I hope it is soon. People need the help.

CYBER SECURITY

Mr. President, in the last few days we have learned that the United States was subject to one of the most brazen cyber hacks in history. Based on press reports alone, the hackers appear to have breached the Department of State, the Department of Commerce, the Department of Energy, the Department of the Treasury, the National Nuclear Security Agency, and the Department of Homeland Security—including the agency responsible for our cyber security.

On top of that, the hackers also managed to breach major American companies like Microsoft and compromised several State governments and other foreign governments all at the same time in this process.

While we are learning more about these breaches, the level of resources and sophistication bears all the hallmarks of Russia. Reports suggest that the hackers have been in the system since the spring and perhaps much longer. According to public reports, they may still be in our system tonight.